M. ANDERSON BERRY (262879)
aberry@justice4you.com
LESLIE GUILLON (222400)
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

JOHN A. YANCHUNIS (*Pro Hac Vice forthcoming*)
jyanchunis@ForThe People.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

ALEX PYGIN, an individual and California resident, on behalf of himself and all others similarly situated, Plaintiff, vs. BOMBAS, LLC, SHOPIFY (USA) INC. and SHOPIFY, INC. Defendants.	Case No.: ________________________ **CLASS ACTION COMPLAINT** **1) Negligence;** **2) Negligence per se;** **3) Invasion of Privacy;** **4) Declaratory Relief;** **5) Violation of the California Unfair Competition Law, Business & Professions Code § 17200, *et seq*.;** DEMAND FOR JURY TRIAL

Plaintiff Alex Pygin brings this Class Action Complaint against Bombas, LLC ("Bombas"), Shopify (USA) Inc. and Shopify, Inc. ("Shopify") (collectively, "Defendants"), on behalf of themselves and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Bombas specializes in selling socks through its popular website. For online sales, Bombas uses a third-party ecommerce platform to take customers' personal and payment information. The ecommerce platform is supplied to Bombas by Shopify, a multinational corporation that builds, customizes and maintains proprietary ecommerce platforms for online stores and retail point-of-sale systems. Bombas has been using Shopify Plus since early 2015.

2. On June 3, 2020, Bombas notified customers and state Attorneys General about a widespread data breach that occurred over four years earlier, from November 11, 2016 to February 16, 2017 (the "Data Breach"). Hackers not only "scraped" many of Bombas' customers' names from the website by infecting it with a "malicious code," hackers also stole customers' addresses and payment card information, which likely included payment card numbers, CVV security codes, and payment card expiration dates. The hackers got everything they needed to illegally use Bombas' customers' payment cards to make fraudulent purchases, and to steal the customers' identities.

3. All of this personally identifiable information ("PII") was compromised due to Bombas' and Shopify's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to their failure to prevent the breach, Defendants failed to detect and report the breach for almost four years.

4. Neither Bombas nor Shopify had any idea the breach was happening.[1] In December

[1] *See, e.g.*, Exhibit 1, Bombas' *Notice of Data Breach*, June 3, 2020, archived by the Washington Attorney General, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Safeguarding_Consumers/BombasLLC.2020-06-03.pdf (last accessed June 23, 2020); *see also* Bombas' *Notice of Data Breach*, June 3, 2020, archived by the California Attorney General, *available at*:

2018, Bombas was notified by a third-party that Bombas' customers' PII may have been exposed to hackers. In January 2019, Bombas retained outside legal counsel to further investigate the breach. That investigation revealed that the "malicious code" located in Bombas' Shopify ecommerce platform had not led to a data breach and was not functional. Later in 2019, however, Bombas learned that the same "malicious code" existed on its Shopify ecommerce platform much earlier than Bombas and its counsel first realized.

5. Bombas started another investigation by the same outside counsel. Counsel and its hired experts determined that the "malicious code" it previously reported as "innocuous" was actually operating on Bombas' Shopify ecommerce platform as early as November 11, 2016. In March 2020, counsel determined that Shopify's security features that made the "malicious code" innocuous was not installed on the platform until February 16, 2017. Thus, Bombas could "not rule out the possibility that the malicious code could have successfully scraped customer information between November 11, 2016 and February 16, 2017" before Shopify installed the supposedly effective security features.

6. Bombas did not tell customers or the Attorneys General about this March 2020 discovery until almost three months later, on June 3, 2020. To this day, Shopify has not released a vulnerabilities and exposures report, nor has Shopify made any notifications of the breach.

7. The stolen PII has great value to hackers due to the numbers involved: It is likely that this breach affected over a hundred thousand customers. For example, the Washington State Attorney General reports that 2,313 Washingtonians were affected, the Indiana Attorney General reports that 1,728, and the Iowa Attorney General reports 965 affected citizens.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor Bombas' website and Shopify ecommerce platform for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

https://oag.ca.gov/system/files/Sample%20Individual%20Notice_1.pdf (last accessed on June 23, 2020).

9. Plaintiff and similarly situated Bombas/Shopify customers ("Class members") have suffered injury as a result of Defendants' conduct. These injuries may include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*); (v) the continued and certainly an increased risk to their PII, which (a) may remain available on the dark web for individuals to access and abuse, and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

10. Plaintiff Alex Pygin is a citizen of California residing in Orange County. Mr. Pygin purchased items from Bombas' website between November 11, 2016 to February 16, 2017. He received Bombas' *Notice of Data Breach*, dated June 1, 2020, on or about June 3, 2020.

11. Defendant Bombas, LLC is a New York Limited Liability Company with its principal place of business located at 37 East 18th Street, 4th Floor, New York, New York. During the class period, Bombas operated across the United States through its website, and sold socks and other clothing at various retailers throughout California.

12. On information and belief, Defendant Shopify (USA) Inc. is a Delaware company with its principal place of business in San Francisco, California, previously acquired and/or created by Shopify Inc. and jointly responsible for the wrongful activities alleged herein with respect to Shopify's conduct in the United States.

13. On information and belief, Defendant Shopify, Inc. is a Canadian company with its principal place of business in Ontario, Canada, which previously acquired and/or created Shopify (USA) Inc. and is jointly responsible for the wrongful activities alleged herein with respect to Shopify's conduct in the United States.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant Bombas. Moreover, Plaintiff is a California citizen and therefore diverse from Bombas, which is headquartered in New York.

15. This Court has personal jurisdiction over Defendants because Bombas and Shopify have systematic and continuous contacts with the state of California through their websites.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant Shopify (USA) Inc. resides within this judicial district and substantial part of the events giving rise to the claims alleged herein occurred within this judicial district, specifically Defendants' business with online retailers, including many located within this judicial district.

IV. FACTUAL ALLEGATIONS

Bombas Background

17. Bombas has sold socks and a limited selection of clothing through its website, www.bombassocks.com, and other retailers since 2013. By 2018, the company reported revenue exceeding $100 million.

18. Bombas ensures its customers that it is concerned about PII security:

> Bombas has developed this **Bombas LLC Privacy Policy and Cookie Policy** (the "Privacy Policy") to demonstrate its commitment to protecting the personal and private information of those using the www.bombassocks.com Website (the "Website"). Bombas, including its affiliates, is committed to protecting the privacy of users of our Website (emphasis in original).
>
> …
>
> Bombas will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your personal data will take place to an organization or a country unless there are adequate

controls in place including with respect to the security of your personal data.[2]

19. Bombas does not claim that it abides by the PCI DSS (Payment Card Industry Data Security Standard) compliance, which is a requirement for businesses that store, process, or transmit payment card data. Shopify, however, claims that all of its customers "are PCI compliant by default."[3]

20. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

21. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[4]

22. To purchase items on Bombas' website, customers can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following PII onto the website:

- Name;
- billing address;
- shipping address;
- email address;
- name on the credit card;
- type of credit card;
- full credit card number;
- credit card expiration date; and
- security code, or CVV code (card verification number).

[2] Bombas' *Privacy Policy and Cookies Policy*, *available at*: https://bombas.com/pages/privacy-policy (last accessed June 23, 2020).

[3] Shopify's statement regarding *PCI COMPLIANCE*, *Keep your business and customers secure*, *available at*: https://www.shopify.com/security/pci-compliant (last accessed June 23, 2020).

[4] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed June 23, 2020).

23. When a customer purchases items on Bombas' website, as a guest or through an account, they are not asked to acknowledge the "Privacy Policy," and they are not asked to agree to Bombas' "Terms and Conditions." Links to Bombas' "Privacy Policy" and "Terms and Conditions" are included on the extreme bottom left border of the main website pages in black, unremarkable font, with no indications of hyperlinks to the policies or terms.

24. Bombas migrated its ecommerce platform to Shopify Plus in early 2015.[5]

Shopify Background

25. Shopify offers online retailers a suite of services, including payments, marketing, shipping and customer engagement tools to simplify the process of running an online store. In June 2019, the company reported that it had more than 1,000,000 businesses in approximately 175 countries using its platform, with total gross merchandise volume exceeding $41 billion for calendar year 2018.[6]

26. Shopify Plus, which Bombas has used since February 2015, is one of Shopify's proprietary ecommerce platforms for online stores. Practically, businesses use Shopify Plus to provide user-friendly, secure websites for their customers to purchase items online. The Shopify Plus platform takes the key payment and personal information from the customer to finalize the transaction, including name, billing and shipping addresses, payment card type and number, CVV (security) code, credit card expiration date, email address and sometimes telephone number.

27. Shopify's "Privacy for Customers" policy, directed toward individual customers of the retailers using Shopify Plus, states, "What we collect: Information you provide about yourself like your name, billing address, shipping address, email address, phone number, and payment information." [7]

[5] *See* Exhibit 2, Bombas' *Data Breach Notice to New Hampshire's Attorney General*, Aug. 31, 2018; Shopify's *Shopify Plus Customer page* entitled "Bombas migrated for site stability," *available at*: https://www.shopify.com/plus/customers/bombas (last accessed June 23, 2020).

[6] *Shopify Announces Fourth-Quarter and Full Year 2018 Financial Results*, Businesswire.com, *available at*: https://www.businesswire.com/news/home/20190212005234/en/ (last accessed June 23, 2020).

[7] Exhibit 3, Shopify's *Privacy for Customers* policies, *available at*: https://www.shopify.com/legal/privacy/customers (last accessed June 24, 2020) ("[P]lease review our overall privacy policy that applies to everyone whose information we process.")

28. Retailers and customers demand security to safeguard this sensitive PII. Shopify touts the secure nature of its Shopify Plus ecommerce platform to the retailers, like Bombas:

> Running a secure ecommerce solution and keeping your online store safe is our number one priority. We continuously invest significant time and money to adjust to the latest threats.[8]

29. Shopify expressly states that its "overall privacy policy" applies to not only Bombas and other retail customers, but also to those retailers' individual customers, including Plaintiff and the Class members.[9] That Privacy Policy also touts the secure nature of its Shopify Plus ecommerce platform to customers:

- **"We protect your information from others"**;
- "Our teams work tirelessly to protect your information, and to ensure the security and integrity of our platform. We also have independent auditors assess the security of our data storage and systems that process financial information";
- "When building and improving our products, our engineers work closely with our privacy and security teams to build with privacy in mind. In all of this work our guiding principle is that your information belongs to you";
- **"We help merchants and partners meet their privacy obligations . . . .** To do this, we try to build our products and services so they can easily be used in a privacy-friendly way";
- "We only process personal information for these 'legitimate interests'," including "preventing risk and fraud."[10]

The Data Breach

30. In early June 2020, Bombas sent customers a *Notice of Data Breach*.[11] Bombas' Co-Founder and Chief Executive Officer, David Heath, informed Bombas' affected customers

[8] Shopify's *Shopify Security Response* webpage, *available at*: https://www.shopify.com/security-response (last accessed June 24, 2020).

[9] Exhibit 3.

[10] Exhibit 4, Shopify's *Privacy Policy*, *available at*: https://www.shopify.com/legal/privacy (last accessed June 24, 2020).

[11] Exhibit 1, Bombas' *Notice of Data Breach*, June 3, 2020, pp. 3-7.

that:

> **What Happened?**
> Last year, as part of a review of data security, we discovered that malicious code designed to scrape credit card numbers and other personal information may have been present as early as November 11, 2016 on our e-commerce platform. We launched a thorough investigation to determine whether personal information of our customers was potentially exposed.
>
> On May 20, 2020, we received an investigative report, which could not rule out the possibility that the malicious code could have successfully scraped customer information. The report also confirmed that a new security feature, which was added to our e-commerce platform on February 16, 2017, prevented the malicious code from functioning after that date. Accordingly, there is a window from November 11, 2016 to February 16, 2017 during which customer information potentially could have been exposed.
>
> **What Information Was Involved?**
> We believe that the malicious code could have enabled the attacker to acquire certain personal information belonging to customers who entered their payment card information in our online checkout process during the relevant period. The affected information may have included your name, address, and payment card data.[12]

31. On or about June 3, 2020, Bombas' counsel at Ropes & Gray in Washington, DC, mailed a "Data Incident" letter, attaching the *Notice of Data Breach*, to the Attorneys General of the states where affected customers reside.[13]

32. In the letter sent to the Attorneys General, Bombas revealed even more information about the Data Breach, especially concerning Shopify's involvement:

> On December 26, 2018, Bombas received a Common Point of Purchase (CPP) report from BrainTree,[14] which resulted in a rapid review of its security. By January 3, 2019, Ropes & Gray had been retained and engaged Stroz Friedberg, who had **located and analyzed malicious code operating in its Shopify e-commerce site**. By January 10, 2019, Stroz Friedberg concluded, however, that the malicious code was not functional; and on January 14, 2019, **Shopify assured Bombas that its security features "result in the malware being rendered innocuous**."
>
> In late 2019, as part of a review of data security, **Bombas discovered that the same malicious code designed to scrape credit card numbers and other personal**

[12] *Id* at 3.
[13] *Id*. at 1-2.
[14] Braintree, a division of PayPal, specializes in mobile and web payment systems for ecommerce companies.

> **information may have been present as early as November 11, 2016**. Bombas promptly re-launched a thorough investigation to determine whether personal information of its customers had been potentially exposed by the code that it had been assured was "innocuous" earlier that year.
>
> On May 20, 2020, after extensive investigative work, Stroz Friedberg issued the report of its investigation ("May 2020 Stroz Report"). Like the January 2019 report, the May 2020 Stroz Report found that the Shopify security features prevented the malicious code from functioning. **The May 2020 Stroz Report also found that the Shopify security feature was added to Bombas' e-commerce platform only on February 16, 2017**. Accordingly, the May 2020 Stroz Report could not rule out the possibility that the malicious code could have successfully scraped customer information between November 11, 2016 and February 16, 2017.
>
> The malicious code, when functional, could have enabled the attacker to acquire certain personal information belonging to customers who entered their payment card information in its online checkout process during the relevant period. The affected information may have included customer name, address, and payment card data (emphases added).

33. Although Bombas had been using Shopify Plus since 2015, Shopify did not detect the "malicious code" on its ecommerce platform, and did not add the necessary "security features" until February 16, 2017.

34. Bombas admits that it did not detect the Data Breach either, and did not report it for almost four years. Bombas' customers' information was scraped by hackers and available to other criminals and, on information and belief, may still be for sale to criminals on the dark web. Unauthorized individuals accessed Bombas' customers' unencrypted, unredacted information, including name, address, and payment card information, which includes payment card number, CVV code, expiration date, and possibly more.

Bombas Suffered a Substantially Similar Data Breach Two Years Earlier

35. Not long after this Data Breach occurred in 2016-2017, but before Bombas reported it to its customers and various Attorneys General, Bombas admitted to not reporting a very similar data breach that occurred in 2014.[15] According to New York's Attorney General Letitia James ("NYAG"), Bombas agreed in June 2019 to pay penalties and implement data security policies to

[15] Exhibit 5, New York Attorney General, Press Release, *Attorney General James Announces $65,000 Settlement With Online Retailer Bombas LLC Over Consumer Data Breach*, *available at*: https://ag.ny.gov/press-release/2019/attorney-general-james-announces-65000-settlement-online-retailer-bombas-llc-over (last accessed June 23, 2020); *see also* Exhibit 2.

resolve an investigation by the NYAG into the breach of customer payment cards where Bombas failed to provide notice of the breach to almost 40,000 consumers for over three years.

36. According to the NYAG, on September 27, 2014, "unauthorized intruder(s) inserted malicious software code designed to steal payment card information" into Bombas' ecommerce platform, then maintained and hosted by Magento. The NYAG also reported:

> While Bombas discovered the code on November 29, 2014, it did not remediate it until January 15, 2015. Additionally, the code was mistakenly reintroduced into the website by Bombas a few weeks later. The code was permanently deleted on February 8, 2015. It was determined that the intruders accessed customer information including names, addresses, and credit card information of 39,561 payment card holders– roughly 2,971 of whom were New Yorkers.

37. Similar to the current Data Breach, Bombas did not notify customers right away. In fact, Bombas waited years:

> Bombas LLC began notifying affected consumers in May 2018, more than three years after the company learned of the breach. Because Bombas did not notify the affected consumers and relevant New York agencies in an expedient time-period, and without unreasonable delay, it violated General Business Law §§ 899-aa.

38. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or its backend content management system. Armed with the knowledge in 2018 that hackers scraped Bombas' ecommerce platform in 2014, it is unreasonable that Defendants did not detect the substantially similar 2016-2017 Data Breach at issue here. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be stolen by hackers.

Scraping and E-Skimming Breaches

39. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[16] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the

[16] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed June 24, 2020).

dark web.[17]

40. The hackers target what they refer to as the *fullz*; a term used by criminals to refer to stealing the full primary account number, card holder contact information, credit card number, CVC code and expiration date. The *fullz* is exactly what Bombas admits the malware infecting Shopify's platform scraped.

41. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily comprising the victim website's network or server.[18] These attacks often target third-party payment processors, like Shopify and Salesforce.[19]

42. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[20] Thus, Defendants' would have been made aware of this type of breach before 2016, especially considering the Bombas' 2014 data breach that also involved scraping.

43. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendants' approach to maintaining the privacy and security of Plaintiff's and Class members' PII was negligent, or at the very least, Defendants' did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.

Value of Personally Identifiable Information

44. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[17] *Id.*

[18] *What is Magecart and was it behind the Ticketmaster and BA hacks?*, Computerworld, Sep. 18, 2018, *available at*: https://www.computerworld.com/article/3427858/what-is-magecart-and-was-it-behind-the-ticketmaster-and-ba-hacks-.html (last accessed June 24, 2020).

[19] *Id.*

[20] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed June 23, 2020).

and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

45. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

46. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on its website – the malware infected Shopify's platform during the lead up to Christmas 2016 – amounting to potentially hundreds of thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

Plaintiff's Experience

47. Plaintiff Pygin accessed Bombas' website from his home in California on November 20, 2016 and purchased an eight-pack of Bombas socks for a total of $65.28.

48. Mr. Pygin made this purchase through his Bombas account, which he opened in November 2016. He still has the same credit card account that he used on the Bombas website at that time.

49. Mr. Pygin entered his PII into Defendants' ecommerce payment platform, including his full name, billing and shipping addresses, payment card type and full number, CVV code, credit card expiration date and email address.

50. During this transaction, Mr. Pygin was not asked or directed to "agree" to or even

[21] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 26, 2020).

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 26, 2020).

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 23, 2020).

review Bombas' "Privacy Policy" or "Terms and Conditions."

51. Mr. Pygin received the *Notice of Data Breach*, dated June 1, 2020, on or about June 3, 2020. He did not receive the "Data Incident" letter sent by Bombas to Attorneys General.

52. As a result of the Data Breach notice, Mr. Pygin spent time dealing with the consequences of the breach, which includes time spent confirming that he made a purchase by payment card during the relevant period, reviewing the account compromised by the breach, contacting Bombas and his credit card company, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

53. Mr. Pygin is not aware of any other relevant data breaches that could have resulted in the theft of his credit card information. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

54. Mr. Pygin stores any and all documents containing his PII in a safe and secure digital location, and destroys any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts, using a password manager that generates highly secure, maximum length passwords.

55. Mr. Pygin suffered actual injury and damages in paying money to, and purchasing products from, Defendants' website during the Data Breach; expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

56. Mr. Pygin suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

57. Mr. Pygin suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy.

58. Mr. Pygin has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being placed in the hands of criminals.

59. Mr. Pygin has a continuing interest in ensuring that his PII, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

60. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class: **All individuals whose PII was compromised in the data breach announced by Bombas on June 3, 2020 (the "Nationwide Class").**

61. The California Class is initially defined as follows: **All persons residing in California whose PII was compromised in the data breach announced by Bombas on June 3, 2020 (the "California Class").**

62. Excluded from the Class are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

63. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

64. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the data breach, including approximately over 10,000 in California alone, and the Classes are apparently identifiable within Defendants' records.

65. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. Whether and when Defendants actually learned of the data breach and whether its response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendants caused Plaintiff and Class members damages;

i. Whether Defendants violated the law by failing to promptly notify Class members that their PII had been compromised;

j. Whether Plaintiff and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated California's Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practices;

l. Whether Defendants violated California's California Consumer Privacy Act by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.

66. **Typicality**: Plaintiff's claims are typical of those of other Class members because all had their PII compromised as a result of the data breach, due to Defendants' misfeasance.

67. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's Counsel are competent and experienced in litigating privacy-related

class actions.

68. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

70. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

71. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

72. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

73. The legal duties owed by Defendants to Plaintiff and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in its possession;

b. To protect PII of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

74. In addition, Cal. Civ. Code §1798.81.5 requires Defendants to take reasonable steps and employ reasonable methods of safeguarding the PII of Class members who are California residents.

75. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendants.[24]

[24] Shopify admits that it is subject to the FTC Act ("[W]e are subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission"). Exhibit 4, Shopify's *Privacy Policy*.

76. Various FTC publications and data security breach orders further form the basis of Defendants' duty.[25] Plaintiff and Class members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

77. Defendants breached its duties to Plaintiff and Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that "scraping" hacks were surging in 2016 and on the rise in 2017.

78. Defendants knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendants' ecommerce platform from at least November 11, 2016.

79. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Defendants' possession and control.

80. Defendants breached the duties it owes to Plaintiff and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (*e.g.*, Shopify claims its platform is PCI DSS compliant

[25] *See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 30, 2019), *available at*: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach) (last accessed June 24, 2020).

and encrypts customers' order information, such as name, address, and credit card number, during data transmission, but that did not occur here);

c. Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to E-skimming or similar attacks (*e.g.*, Defendants did not detect the "malicious code" on the ecommerce platform, and Shopify did not add necessary "security features" until February 16, 2017, which should have been added beforehand); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

81. Due to Defendants' conduct, Plaintiff and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers not only "scraped" many of Bombas' customers' names from the website, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and credit card expiration dates. They got the *fullz* – everything they need to illegally use Bombas' customers' credit cards to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

82. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[26] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

83. As a result of Defendants' negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated

[26] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring, but it only monitors victims' credit reports at one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

84. These injuries were reasonably foreseeable given the history of security breaches of this nature, especially considering a substantially similar breach of Bombas' ecommerce platform in 2014. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

85. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

86. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

87. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the

foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Class members.

88. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

89. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

90. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

91. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Breach for the remainder of the lives of Plaintiff and Class members ; and (ix) the diminished value of Defendants' goods and services they received.

92. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

93. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

94. Plaintiff and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

95. Defendants owed a duty to their customers, including Plaintiff and Class members, to keep their PII contained as a part thereof, confidential.

96. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class members.

97. Defendants allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiff and Class members, by way of Defendants' failure to protect the PII.

98. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class members is highly offensive to a reasonable person.

99. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendants as part of their use of Defendants' services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

100. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

101. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that their information security practices were inadequate and insufficient.

102. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

103. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and Class members was disclosed to and used by third parties without authorization, causing Plaintiff and Class members to suffer damages.

104. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

105. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

106. Defendants owe duties of care to Plaintiff and Class members which would require it to adequately secure PII.

107. Defendants still possess PII regarding Plaintiff and Class members.

108. Although Bombas claims it has "taken and is taking steps to protect the security of its customers' information including investments in the people, processes, and technologies that drive its comprehensive information security program," there is little detail on what, if any, fixes have really occurred.

109. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

110. There is no reason to believe that Defendants' security measures are any more adequate than they were before the breach to meet Defendants' contractual obligations and legal duties, and there is no reason to think Defendants have no other security vulnerabilities that have not yet been knowingly exploited.

111. Plaintiff, therefore, seek a declaration that (1) each Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants conduct regular database scanning and securing checks;

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Defendants to purchase credit monitoring services for Plaintiff and Class members for a period of ten years; and

h. Ordering Defendants to meaningfully educate its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants customers must take to protect themselves.

COUNT V
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 – Unlawful Business Practices
(On Behalf of Plaintiff and the Nationwide Class Or, in the Alternative, On Behalf of Plaintiff and the California Class)

112. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

113. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Class.

114. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Nationwide and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and the Nationwide and California Class members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiff and the Nationwide and California Class members.

115. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to Nationwide and California Class members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant Shopify has still not provided such information to Plaintiff and the Nationwide and California Class members.

116. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiff and the Nationwide and California Class members were injured and lost money or

property, including but not limited to the price received by Defendants for the services, the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

117. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard Nationwide and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Class.

118. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Nationwide and California Class members of money or property that Defendants may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VI
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 – Unfair Business Practices
(On Behalf of Plaintiff and the Nationwide Class, Or in the Alternative, On Behalf of Plaintiff and the California Class)

119. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

120. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and the Nationwide and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Nationwide and California Class members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Nationwide and California Class members. They were likely to deceive the public into believing

their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Nationwide and California Class members outweighed their utility, if any.

121. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Nationwide and California Class members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Nationwide and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Nationwide and California Class members outweighed their utility, if any.

122. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiff and the Nationwide and California Class members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

123. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard the Nationwide and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Classes.

124. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the Nationwide and California Class members of money or property that the Defendants may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

//

//

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class members, request judgment against the Defendants and that the Court grant the following:

A. An order certifying the Nationwide Class and California Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: July 1, 2020

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. ANDERSON BERRY
aberry@justice4you.com
LESLIE GUILLON
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

JOHN A. YANCHUNIS (*Pro Hac Vice*)
jyanchunis@ForThePeople.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402